

High-bit-rate quantum key distribution with entangled internal degrees of freedom of photons

Isaac Nape,¹ Bienvenu Ndagano,¹ Benjamin Perez-Garcia,^{1,2} Stirling Scholes,¹

Raul I. Hernandez-Aranda,² Thomas Konrad,³ and Andrew Forbes^{1,*}

¹*School of Physics, University of the Witwatersrand, Private Bag 3, Wits 2050, South Africa*

²*Photonics and Mathematical Optics Group, Tecnológico de Monterrey, Monterrey 64849, Mexico*

³*College of Chemistry and Physics, University of KwaZulu-Natal,*

Private Bag X54001, Durban 4000, South Africa

(Dated: December 30, 2016)

Quantum communication over long distances is integral to information security and has been demonstrated in free space and fibre with two-dimensional polarisation states of light. Although increased bit rates can be achieved using high-dimensional encoding with spatial modes of light, the efficient detection of high-dimensional states remains a challenge to realise the full benefit of the increased state space. Here we exploit the entanglement between spatial modes and polarization to realise a four-dimensional quantum key distribution (QKD) protocol. We introduce a detection scheme which employs only static elements, allowing for the detection of all basis modes in a high-dimensional space deterministically. As a result we are able to realise the full potential of our high-dimensional state space, demonstrating efficient QKD at high secure key and sift rates, with the highest capacity-to-dimension reported to date. This work opens the possibility to increase the dimensionality of the state-space indefinitely while still maintaining deterministic detection and will be invaluable for long distance “secure and fast” data transfer.

I. INTRODUCTION

The use of polarization encoded qubits has become ubiquitous in quantum communication protocols with single photons [1–4]. Most notably, they have enabled unconditionally secure cryptography protocols through quantum key distribution (QKD) over appreciable distances [5–7]. With the increasing technological prowess in the field, faster and efficient key generation together with robustness to third party attacks have become paramount issues to address. A topical approach to overcome these hurdles is through higher-dimensional QKD: increasing the dimensionality, d , of a QKD protocol leads to better security and higher secure key rates, with each photon carrying up to $\log_2(d)$ bits of information [8, 9].

Employing spatial modes of light, particularly those carrying orbital angular momentum (OAM), has shown considerable improvements in data transfer of classical communication systems [10–12]. However, realizing high-dimensional quantum communication remains challenging. To date, the list of reports on high dimensional QKD with spatial modes is not exhaustive, and include protocols in up to $d = 7$ [13–15]. It is worth noting that due to experimental limitations, the secret key rate of a given QKD protocol does not scale with the dimension, i.e., given a certain set of experimental parameters there exist an optimum number of dimension that maximizes the secret key rate [16].

Photons with complex spatial and polarization structure, commonly known as vector modes, have been used as information carriers for polarisation encoded qubits

in alignment-free QKD [17, 18], exploiting the fact that vector modes that carry OAM exhibit rotational symmetry, removing the need to align the detectors in order to reconcile the encoding and decoding bases, as would be the case in QKD with only polarization. In these vector modes, the spatial and polarization degrees of freedom (DoFs) are coupled in a non-separable manner, reminiscent of entanglement in quantum mechanics. This non-separability can be used to encode information and has been done so with classical light [19, 20], for example, in mode division multiplexing [21].

Here we use the non-separability of vector OAM modes (vector vortex modes) to realize four-dimensional QKD based on the “BB84” protocol [22]. Rather than carrying information encoded in one DoF, the non-separable state can itself constitute a basis for a higher dimensional space that combines two DoFs, namely the spatial and polarisation DoFs. To fully benefit from the increased state space, we introduce a new detection scheme that, deterministically and without dimension dependent sifting loss, can detect all basis elements in our high-dimensional space. This differs from previous schemes that have used mode filters as detectors, sifting through the space one mode at a time, thus removing all benefit of the dimensionality of the space (see for example ref. [14]). Our approach combines manipulations of the dynamic and Pancharatnam-Berry phase with static optical elements and, in principle, allows detection of the basis elements with unit probability. We demonstrate high-dimensional encoding/decoding in our entangled space, obtaining a detection fidelity as high as 97%, with a secret key rate of 1.63 bits per photon and quantum error rate of 3%. As a means of comparison to other protocols, we calculated the capacity-to-dimension ratio and show that our

* Corresponding author: andrew.forbes@wits.ac.za

scheme is more efficient than any other reported to date.

II. RESULTS

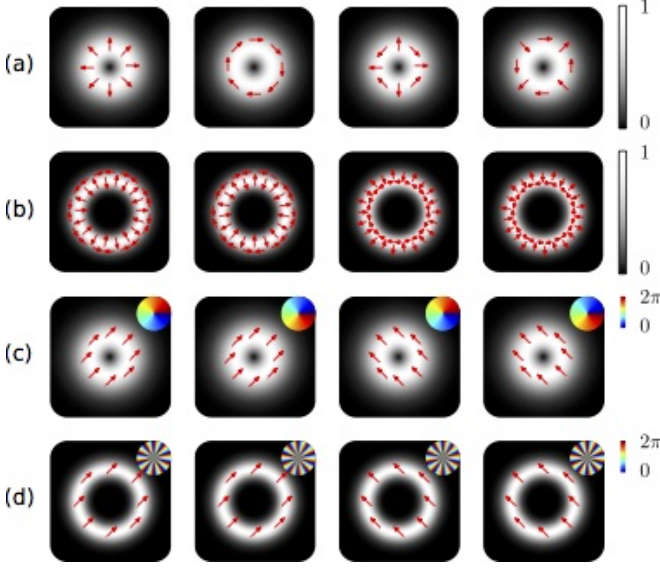


FIG. 1. **Modes in a four-dimensional hyper-entangled space.** Vector vortex modes for (a) $\ell = \pm 1$ and (b) $\ell = \pm 10$, with the mutually unbiased scalar modes also for the (c) $\ell = \pm 1$ and (d) $\ell = \pm 10$ subspaces. The insets show the azimuthally varying phase profile of the scalar modes.

High-dimensional encoding. The first QKD demonstrations were performed using the polarisation DoF, namely, states in the space spanned by left-circular $|L\rangle$ and right-circular polarization $|R\rangle$, i.e., $\mathcal{H}_\sigma = \text{span}\{|L\rangle, |R\rangle\}$, and later using the spatial mode of light as a DoF, e.g., space spanned by the OAM modes $|\ell\rangle$ and $|\ell\rangle$, i.e. $\mathcal{H}_\ell = \text{span}\{|\ell\rangle, |-\ell\rangle\}$. Using entangled states in both DoFs allows one to access an even larger state space, i.e., $\mathcal{H}_\Omega = \mathcal{H}_\sigma \otimes \mathcal{H}_\ell$, described by the higher-order Poincaré sphere [23, 24]. When many ℓ subspaces are combined, the dimension d of the final space incorporating N OAM values ($\ell \in \Omega \subset \mathbf{N}$) is given by $d = 4N$. This opens the way to infinite dimensional encoding using such hyper-entangled states.

For example, using only the $|\ell|$ subspace of OAM ($N = 1$) leads to a four dimensional space spanned by $\{|\ell, L\rangle, |-\ell, L\rangle, |\ell, R\rangle, |-\ell, R\rangle\}$. It is precisely in this four-dimensional subspace that, here, we define our vector and scalar modes. Alice randomly prepares photons in modes from two sets: a vector mode set, $|\psi\rangle_{\ell,\theta}$, and a mutually unbiased scalar mode set, $|\phi\rangle_{\ell,\theta}$, defined as

$$|\psi\rangle_{\ell,\theta} = \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + e^{i\theta}|L\rangle|-\ell\rangle), \quad (1)$$

$$|\phi\rangle_{\ell,\theta} = \frac{1}{\sqrt{2}}(|R\rangle + e^{i(\theta-\frac{\pi}{2})}|L\rangle)|\ell\rangle, \quad (2)$$

where each photon carries $\ell\hbar$ quanta of OAM, $|R\rangle$ and $|L\rangle$ are, respectively, the right and left circular polarization

eigenstates and $\theta = [0, \pi]$ is the intra-modal phase. For a given $|\ell|$ OAM subspace, there exist four orthogonal modes in both the vector basis (Eq. 1) and its mutually unbiased counterpart (Eq. 2), such that $|\langle\psi|\phi\rangle|^2 = 1/d$ with $d = 4$. These vector and scalar modes can be generated by manipulating the dynamic or geometric phase of light [25–28]. Here we employ geometric phase control through a combination of q -plates [29, 30] and wave plates to create all vector and scalar modes in the four dimensional space (see Methods and Supplementary Information). Our four vector modes for QKD then become:

$$|00\rangle = \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + |L\rangle|-\ell\rangle), \quad (3)$$

$$|01\rangle = \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle - |L\rangle|-\ell\rangle), \quad (4)$$

$$|10\rangle = \frac{1}{\sqrt{2}}(|L\rangle|\ell\rangle + |R\rangle|-\ell\rangle), \quad (5)$$

$$|11\rangle = \frac{1}{\sqrt{2}}(|L\rangle|\ell\rangle - |R\rangle|-\ell\rangle), \quad (6)$$

with corresponding MUBs

$$|00\rangle = \frac{1}{\sqrt{2}}|D\rangle|-\ell\rangle, \quad (7)$$

$$|01\rangle = \frac{1}{\sqrt{2}}|D\rangle|\ell\rangle, \quad (8)$$

$$|10\rangle = \frac{1}{\sqrt{2}}|A\rangle|-\ell\rangle, \quad (9)$$

$$|11\rangle = \frac{1}{\sqrt{2}}|A\rangle|\ell\rangle, \quad (10)$$

where D and A refer to diagonal and anti-diagonal polarisation states. For the purpose of demonstration, we use vector and scalar modes in the $\ell = \pm 1$ and $\ell = \pm 10$ OAM subspaces, shown graphically in Fig. 1.

High-dimensional decoding. At the receiver's end, Bob randomly opts to measure the received photon in either the scalar or vector basis. The randomness of the choice between the two bases is implemented here with a 50:50 beam splitter (BS) as shown in Fig. 2(a). Prior QKD experiments beyond two-dimensions have used filtering based techniques that negate the very benefit of the increased state space: by filtering for only one mode at a time, the effective data transfer rate is reduced by a factor $1/d$. We introduce a new scheme to deterministically detect the modes, as detailed in Fig. 2 (b) and (c), that has a number of practical advantages for quantum cryptography. Consider a vector mode as defined in Eq. 1. The sorting of the different vector modes is achieved through a combination of geometric phase control and multi-path interference. First, a polarisation grating based on geometric phase acts as a beam splitter for left- and right-circularly polarised photons, creating two paths

$$|\Psi\rangle_{\ell,\theta} \rightarrow \frac{1}{\sqrt{2}}(|\ell\rangle_a |R\rangle_a + e^{i\theta}|-\ell\rangle_b |L\rangle_b), \quad (11)$$

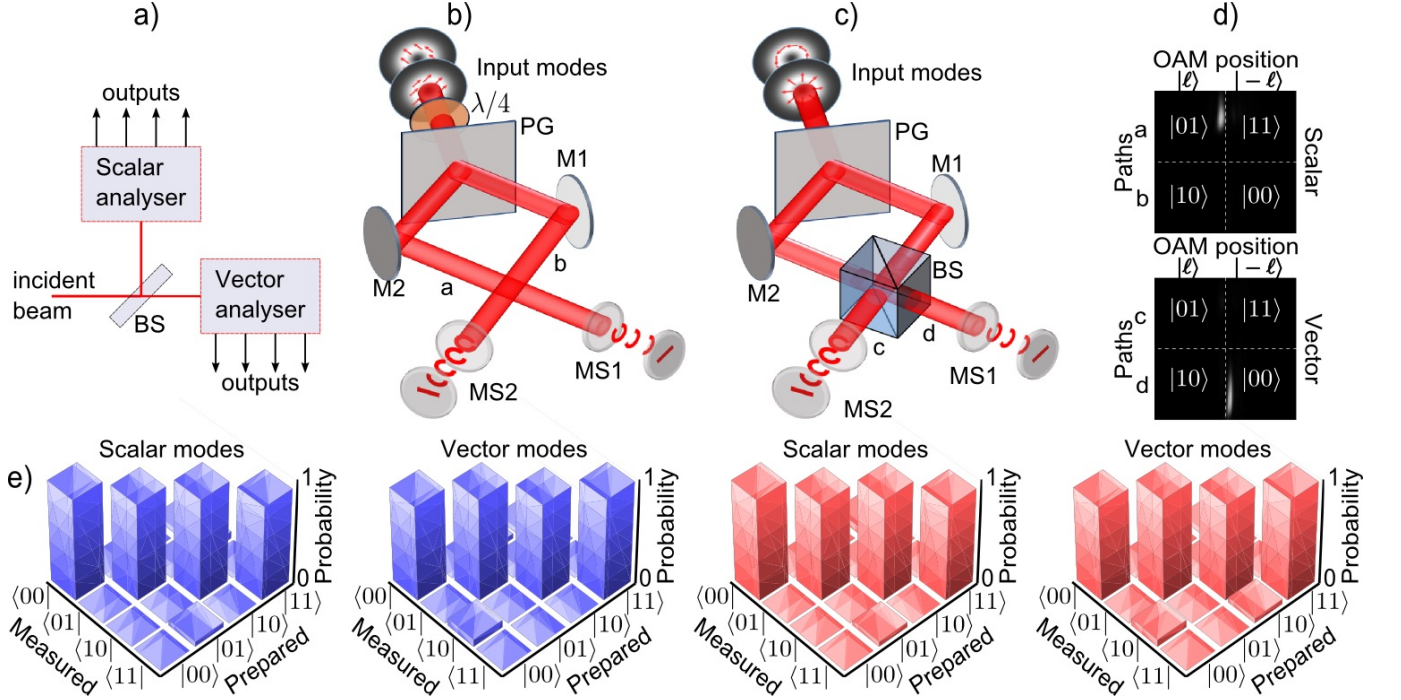


FIG. 2. **Deterministic detection of the full state space.** (a) Bob randomly selects to measure the incoming single photon from Alice in either the $|\psi\rangle_\ell$ (vector) or $|\phi\rangle_\ell$ (scalar) basis and detects the photon deterministically with eight detection ports. (b) The $|\phi\rangle_\ell$ scalar analyser first convert linear to circular polarisation using a quarter-wave plate, then polarisation to path with a polarisation grating (PG). Subsequently the OAM states are measured using mode sorters (MS1 and MS2) that map OAM to position. (c) The $|\psi\rangle_\ell$ vector analyser works in analogous fashion, with the exception that the paths after the PG are interfered on a beam-splitter (BS) before passing the resulting output from each port to an OAM detector (mode sorter). (d) The inputs states prepared by Alice are now unambiguously mapped to detectors in Bob's measurement system, allowing all states to be detected with the eight detectors. Experimental data is shown for two of the cases. (e) Experimental confirmation of Bob's detection scheme for both $|\psi\rangle_\ell$ and $|\phi\rangle_\ell$ states prepared by Alice, for $\ell = \pm 1$ (blue) and $\ell = \pm 10$ (red).

where the subscript a and b refer to the polarisation-marked paths. The photon paths a and b are interfered at a 50:50 BS, resulting in the following state after the BS:

$$|\Psi'\rangle_{\ell,\theta} = \frac{1 + e^{i(\delta+\theta+\frac{\pi}{2})}}{2} |\ell\rangle_c + i \frac{1 + e^{i(\delta+\theta-\frac{\pi}{2})}}{2} |-\ell\rangle_d \quad (12)$$

where the subscripts c and d refer to the output ports of the beam splitter and δ is the dynamic phase difference between the two paths. Note that the polarisation of the two paths is automatically reconciled in each of the output ports of the beam splitter due to the difference of parity in the number of reflections for each input arm. Also note that at this point it is not necessary to retain the polarisation kets in the expression of the photon state since the polarisation information is contained in the path. In our setup we set $\delta = \pi/2$, reducing the state in Eq. 12 to

$$|\Psi'\rangle_{\ell,\theta} = \frac{1 - e^{i\theta}}{2} |\ell\rangle_c + i \frac{1 + e^{i\theta}}{2} |-\ell\rangle_d \quad (13)$$

The measurement system is completed by passing each of the outputs in c and d through a mode sorter and collecting the photons using 4 multimode fibres coupled

to avalanches photodiodes. The mode sorters are refractive (lossless) aspheres that map OAM to position [31–34] (see Supplementary Information for a layout of the detection system). While it is trivial to measure such hyper-entangled (non-separable) vector states at the classical level [19, 21, 35], with our approach each such state is detected with unit probability at the single photon level. For example, consider the modes $|00\rangle$ and $|01\rangle$, where $\theta = 0$ and $\theta = \pi$, respectively. The mapping is such that

$$|00\rangle \rightarrow |\Psi'\rangle_{\ell,0} = i |-\ell\rangle_d, \quad (14)$$

$$|01\rangle \rightarrow |\Psi'\rangle_{\ell,\pi} = -|\ell\rangle_c. \quad (15)$$

The combination of path (c or d) and lateral location ($+\ell$ or $-\ell$) uniquely determines the original vector mode as shown in Fig. 2(d)

The scalar mode detector works on an analogous principle but without the need of the BS to resolve the intermodal phases (see Supplementary Information). The polarisation states are resolved by first performing a unitary transformation that maps linear to circular basis, and passing the scalar mode through the polarisation grating. The OAM states are subsequently sorted using the mode sorters.

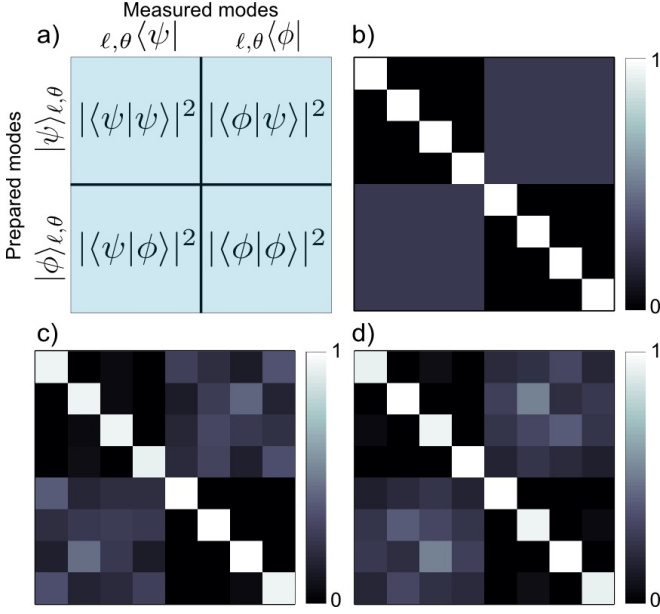


FIG. 3. **Crosstalk analysis in four dimensions.** (a) Schematic of the inner product measurements performed between the vector states $|\psi\rangle_{\ell,\theta}$ and their mutually unbiased counterparts $|\phi\rangle_{\ell,\theta}$. (b) Theoretical scattering probabilities among the vector and scalar modes following the measurement process of (a). The experimental results are shown in (c) and (d) for modes in the $\ell = \pm 1$ and $\ell = \pm 10$ subspaces, respectively.

A graphical illustration of the experimental performance of both the scalar and vector analysers is shown in Fig. 2(e), where modes from the $\ell = \pm 1$ and $\ell = \pm 10$ subsets were measured with high fidelity (close to unity).

High dimensional cryptography. We performed a four-dimensional prepare-and-measure BB84 scheme [22] using mutually unbiased vector and scalar modes. Light from our source was attenuated to the single photon level with an average photon number of $\mu = 0.008$. Alice prepared an initial state in either the $|\psi\rangle_{\ell}$ (vector) or $|\phi\rangle_{\ell}$ (scalar) basis and transmitted it to Bob, who made his measurements as detailed in the previous section. Through optical projection onto both the vector and scalar bases as laid out in Fig. 3(a), we determined the crosstalk matrices shown in Fig. 3(c) and (d), relating the input and measured modes within, respectively, the subspaces $\ell = \pm 1$ and $\ell = \pm 10$. The average fidelity of detection, measured for modes prepared and detected in identical bases, is 0.965 ± 0.004 while the overlap between modes from MUBs is $|\langle\phi|\psi\rangle|^2 = 0.255 \pm 0.004$, in good agreement with theory (0.25).

From the measured crosstalk matrices in Fig. 3(c) and (d), we performed a security analysis on our QKD scheme in dimensions $d = 4$ for the two OAM subspaces (± 1 and ± 10). The results of the analysis are summarised in Table I. From the measured detection fidelity F , we computed the mutual information between Alice and Bob

TABLE I. Summary of the security analysis on the high dimensional protocol showing the experimental and theoretical values of the detection fidelity (F), mutual information I_{AB} between Alice and Bob, Eve's cloning fidelity (F_E) and mutual information with Alice I_{AE} , as well as the quantum error rate Q and secret key rate R .

	$d = 4$ ($ \ell = 1$)	$d = 4$ ($ \ell = 10$)	
Measures	experiment	experiment	ideal
F	0.96	0.97	1.00
I_{AB}	1.69	1.76	2.00
F_E	0.44	0.41	0.25
I_{AE}	0.17	0.13	0.00
Q	0.04	0.03	0.00
R	1.52	1.63	2.00

in d -dimensions as follows [9]

$$I_{AB} = \log_2(d) + F \log_2(F) + (1 - F) \log_2\left(\frac{1 - F}{d}\right). \quad (16)$$

The measured I_{AB} for $d = 4$ is nearly double ($1.7\times$) that of the maximum achievable with only qubit states (1). Assuming a third party, Eve, uses an ideal quantum cloning machine to extract information, the associated cloning fidelity, F_E , in d -dimensions is given by [9]

$$F_E = \frac{F}{d} + \frac{(d - 1)(1 - F)}{d} + \frac{2\sqrt{(d - 1)F(1 - F)}}{d}. \quad (17)$$

With increasing dimensions, the four dimensional protocol reduces the efficiency of Eve's cloning machine to as low as 0.41 well below the maximum limit in a the two-dimensional protocol (0.5). Thus, increasing the dimensionality of QKD protocols does indeed have, in addition to higher mutual information capacity, higher robustness to cloning based attacks.

The mutual information shared between Alice and Bob, conditioned on Bob's error – that is, Bob making a wrong measurement is as a result of Eve extracting the correct information – is computed in d -dimension as follows [9]

$$I_{AE} = \log_2(d) + (F + F_E - 1) \log_2\left(\frac{F + F_E - 1}{F}\right) + (1 - F_E) \log_2\left(\frac{1 - F_E}{(d - 1)F}\right). \quad (18)$$

The consequent measured quantum error rate of $Q = 1 - F = 0.04$ is well below the 0.11 and 0.18 bounds for unconditional security against coherent attacks in two and four dimensions [9], respectively. The lower bound on the secret key rate, $R = \max(I_{AB} - I_{AE}, I_{AB} - I_{BE})$ [36], yields a value as high as 1.63 bits per photon, well above the Shannon limit of one bit per photon achievable with qubit states. While the security of the protocol can be increase with privacy amplification, the measured four-dimensional secret key rate demonstrates the potential of such hyper-entangled modes for high bandwidth quantum communication.

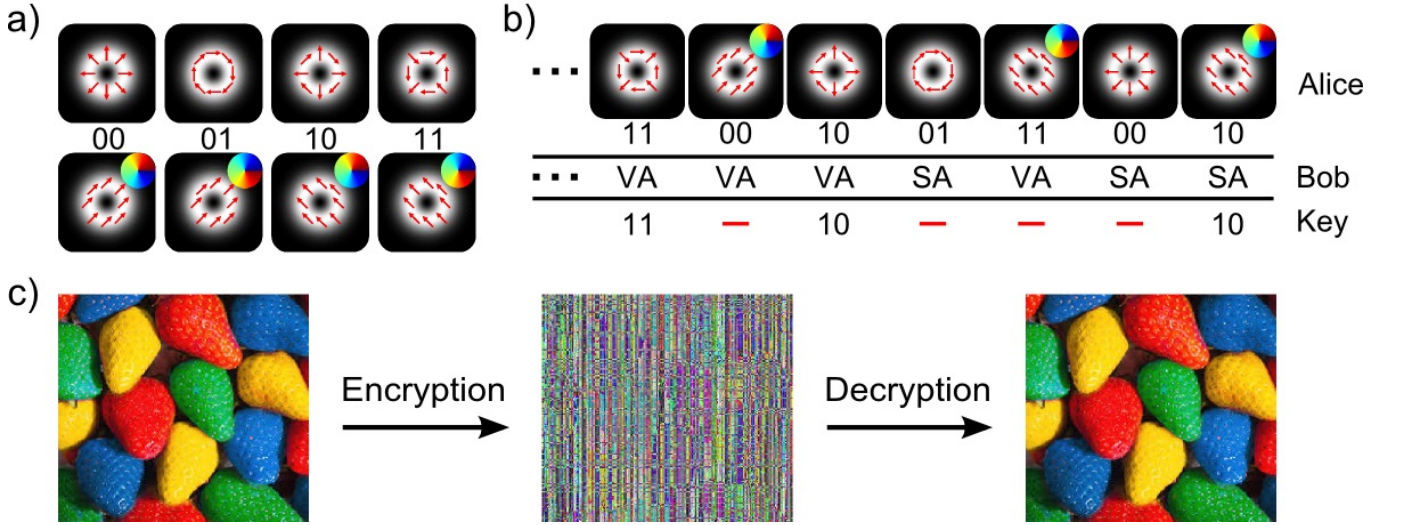


FIG. 4. **High dimensional BB84.** Alice and Bob agree on bit values for the vector and scalar modes. (b) Alice sends a random sequence of vector and scalar modes, which Bob randomly measures using either a vector analyser (VA) or a scalar analyser (SA). Alice and Bob, upon communication of the encoding and decoding bases through a classical channel, discard bit values for modes prepared and measured in complementary bases. (c) Shows a simple encryption/decryption of an image using a 98 bit long key, sifted from a total of 200 transmitted bits.

Finally, we performed a four dimensional prepare-and-measure BB84 scheme using mutually unbiased vector and scalar modes. For each mode, Alice and Bob assign the bit values 00, 01, 10 and 11, as shown in Fig. 4(a). During the transmission, Alice randomly prepares her photon in a vector (scalar) mode state while Bob randomly measures the photon with either the vector or scalar analyser detailed in Fig. 2. At the end of the transmission, Alice and Bob reconcile the prepare and measure bases and discard measurements in complementary bases, as described in Fig. 4(b). We performed this transmission using a sequence of 100 modes and retained a sifted key of 49 spatial modes (98 bits), which was used to encrypt and decrypt a picture as shown in Fig. 4(c).

III. DISCUSSION AND CONCLUSION

The prepare-and-measure quantum cryptography scheme we report here realised the potential of hyper-entanglement between spatial modes and polarisation as means to achieving higher bandwidth optical communication at the single photon level as well as classically. Our secret key rate of 1.63 bits per photon represents a significant increase in data transfer rates as compared to QKD with conventional polarisation eigenstates, limited to one bit per photon under ideal conditions. The secret key rate we obtained exceeds previously reported [14] $d = 4$ laboratory results by more than 43%. In order to compare the efficiency of higher-dimensional protocols we define the information per photon per dimension as a figure of merit. Using this, we find that we achieve a value of 0.41, compared to reported values of 0.17 ($d = 5$) [14] and 0.24 ($d = 7$) [15], highlighting the efficiency of our scheme.

An important aspect of our scheme is the deterministic measurement of all higher dimensional states, allowing, in principle, unit detection probability by Bob for any prepared mode by Alice. This makes it possible to increase the dimensionality of quantum cryptography protocols without compromising on the sifting rate, the fraction of the transmitted bits that constitute the key, unlike with other methods where the data transfer rate is decreased due to filtering for one mode at a time, thereby decreasing the detection probability for a given mode by a factor $1/d$. As a consequence our sift rate is two times greater than would be possible with conventional probabilistic (filtering-based) detection schemes (See Supplementary Information for an experimental comparison). We point out that our scheme would likewise increase the signal-to-noise of classical mode division multiplexing communication systems: rather than distribute the signal across d modes, each with $1/d$ of the signal, we can achieve full signal on each mode with a factor d greater signal-to-noise ratio [37].

In conclusion, we have demonstrated a four-dimensional QKD protocol using a deterministic detection scheme that realises the full benefit of the dimensionality of the state space. Using modes with entangled spatial and polarisation DoFs, we demonstrated the efficiency of the approach using the BB84 scheme. The system performance confirms that the QKD protocol is capable of realising high-bits per photon at high sift rates and high data transfer rates, substantially improving on previously reported results. It is anticipated that, due to the identical scattering of vector and scalar OAM modes in turbulence [38], no benefit will be derived to Eve (mutual information between Bob/Alice and Eve) from this mode set. When combined with real-time error correction [26] and the possibility to increase the dimensionality

of the state-space indefinitely while still maintaining unit probability detection, we foresee that this approach will be invaluable for long distance “secure and fast” data transfer.

IV. METHODS

Generating vector and scalar modes using a q -plate. We used q -plates to couple the polarisation and orbital angular momentum degrees of freedom through geometric phase control. With locally varying birefringence across a wave plate, the geometric phase imparted by a q -plate was engineered to produce the following transformation

$$|\ell, L\rangle \xrightarrow{q\text{-plate}} |\ell + 2q, R\rangle, \quad (19)$$

$$|\ell, R\rangle \xrightarrow{q\text{-plate}} |\ell - 2q, L\rangle, \quad (20)$$

where $q = 2\ell$ is the topological charge of the q -plate. The vector modes investigated here were generated by transforming an input linearly polarised Gaussian mode with quarter- or half-wave plates and $q = 1/2$ and $q = 5$ plates, producing either separable (scalar) non-separable (vector) superpositions of qubit states in Eqs. 19 and 20. The generated states and the elements setting are given in the table below:

TABLE II. Generation of MUBs of vector and scalar modes from an input, horizontally polarised Gaussian beam

Mode	$\lambda/4(\alpha_1)$	$\lambda/2(\theta_1)$	q -plate	$\lambda/4(\alpha_2)$	$\lambda/2(\theta_2)$
$ \psi\rangle_{\ell,0}$	—	0	$ q\rangle$	—	—
$ \psi\rangle_{\ell,\pi}$	—	$\pi/4$	$ q\rangle$	—	—
$ \psi\rangle_{-\ell,0}$	—	—	$ q\rangle$	—	0
$ \psi\rangle_{-\ell,\pi}$	—	—	$ q\rangle$	—	$\pi/4$
$ \phi\rangle_{\ell,0}$	$-\pi/4$	—	$ q\rangle$	$-\pi/4$	$\pi/4$
$ \phi\rangle_{\ell,\pi}$	$-\pi/4$	—	$ q\rangle$	$-\pi/4$	$-\pi/4$
$ \phi\rangle_{-\ell,0}$	$\pi/4$	—	$ q\rangle$	$\pi/4$	$\pi/4$
$ \phi\rangle_{-\ell,\pi}$	$\pi/4$	—	$ q\rangle$	$\pi/4$	$-\pi/4$

-
- [1] H. Hübel, M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe, and A. Zeilinger, *Opt. Express* **15**, 7853-7862 (2007).
- [2] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, *Nat. Phys.* **3**, 481-486 (2007).
- [3] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, *Nat.* **489**, 269-73 (2012).
- [4] T. Herbst, T. Scheidl, M. Fink, J. Handsteiner, B. Wittmann, R. Ursin, and A. Zeilinger, *Proc. Natl. Acad. Sci. USA* **112**, 14202-14205 (2015).
- [5] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, *Phys. Rev. Lett.* **84**, 4729 (2000).
- [6] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Böhm, T. Lorünser, O. Maurhardt, M. Peev, M. Suda, C. Kurtz, H. Weinfurter, T. Jennewein, and A. Zeilinger, *Opt. Express* **12**, 3865-3871 (2004).
- [7] C. Z. Peng, J. Zhang, D. Yang, W. B. Gao, H. X. Ma, H. Yin, H. P. Zeng, T. Yang, X. B. Wang, and J. W. Pan, *Phys. Rev. Lett.* **98**, 010505 (2007).
- [8] H. Bechmann-Pasquinucci and W. Tittel, *Phys. Rev. A* **61**, 062308 (2000).
- [9] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [10] J. Wang, J.-Y. Yang, I. M. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. Ren, Y. Yue, S. Dolinar, M. Tur, and A. E. Willner, *Nat. Phot.* **6**, 488-496 (2012).
- [11] V. Sleiffer, Y. Jung, V. Veljanovski, R. van Uden, M. Kuschnerov, H. Chen, B. Inan, L. G. Nielsen, Y. Sun, D. Richardson, S. Alam, F. Poletti, J. Sahu, A. Dhar, A. Koonen, B. Corbett, R. Winfield, A. Ellis, and H. de Waardt, *Opt. Express* **20**, B428-B438 (2012).
- [12] H. Huang, G. Xie, Y. Yan, N. Ahmed, Y. Ren, Y. Yue, D. Rogawski, M. J. Willner, B. I. Erkmen, K. M. Birnbaum, S. J. Dolinar, M. P. J. Lavery, M. J. Padgett, M. Tur, and A. E. Willner, *Opt. Lett.* **39**, 197-200 (2014).
- [13] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, *New J. Phys.* **8** 75 (2006).
- [14] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, *Phys. Rev. A* **88**, 032305 (2013).
- [15] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. OSullivan, B. Rodenburg, M. Malik, M. P. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, *New J. Phys.* **17**, 033033 (2015).
- [16] J. Leach, E. Bolduc, D. J. Gauthier, and R. W. Boyd, *Phys. Rev. A* **85**, 060304 (2012).
- [17] C. Souza, C. Borges, a. Khoury, J. Huguenin, L. Aolita, and S. Walborn, *Phys. Rev. A* **77**, 032345 (2008).
- [18] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, *Phys. Rev. Lett.* **113**, 060503 (2014).
- [19] G. Milione, T. A. Nguyen, J. Leach, D. A. Nolan, and R. R. Alfano, *Opt. Lett.* **40**, 4887-4890 (2015).
- [20] P. Li, B. Wang, and X. Zhang, *Opt. Express* **24**, 15143-15159 (2016).
- [21] G. Milione, M. P. J. Lavery, H. Huang, Y. Ren, G. Xie, T. A. Nguyen, E. Karimi, L. Marrucci, D. A. Nolan, R. R. Alfano, and A. E. Willner, *Optics letters* **40**, 1980-1983 (2015).
- [22] C. H. Bennett, In *International Conference on Computer System and Signal Processing, IEEE, 1984*, 175-179 (1984).
- [23] G. Milione, H. I. Sztul, D. A. Nolan, and R. R. Alfano, *Phys. Rev. Lett.* **107**, 053601 (2011).

- [24] G. Milione, S. Evans, D. A. Nolan, and R. R. Alfano, *Phys. Rev. Lett.* **108**, 190401 (2012).
- [25] A. Forbes, A. Dudley, and M. McLaren, *Adv. Opt. Phot.* **8**, 200-227 (2016).
- [26] B. Ndagano, B. Perez-Garcia, F. S. Roux, M. McLaren, C. Rosales-Guzman, Y. Zhang, O. Mouane, R. I. Hernandez-Aranda, T. Konrad, and A. Forbes, *arXiv:1605.05144* (2016).
- [27] D. Naidoo, F. S. Roux, A. Dudley, I. Litvin, B. Piccirillo, L. Marrucci, and A. Forbes, *Nat. Phot.* **10**, 327-332 (2016).
- [28] T. H. Lu, T. D. Huang, J. G. Wang, L. W. Wang, and R. R. Alfano, *Sci. Rep.* **6**, 39657 (2016).
- [29] L. Marrucci, C. Manzo, and D. Paparo, *Phys. Rev. Lett.* **96**, 163905 (2006).
- [30] L. Marrucci, E. Karimi, S. Slussarenko, B. Piccirillo, E. Santamato, E. Nagali, and F. Sciarrino, *J. Opt.* **13**, 064001 (2011).
- [31] G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, *Phys. Rev. Lett.* **105**, 153601 (2010).
- [32] R. Fickler, R. Lapkiewicz, M. Huber, M. P. Lavery, M. J. Padgett, and A. Zeilinger, *Nat. Commun* **5**, 4502 (2014).
- [33] M. P. J. Lavery, D. J. Robertson, A. Sponselli, J. Courtial, N. K. Steinhoff, G. A. Tyler, A. E. Wilner, and M. J. Padgett, *New J. Phys.* **15**, 013024 (2013).
- [34] A. Dudley, T. Mhlanga, M. P. J. Lavery, A. McDonald, F. S. Roux, M. Padgett, and A. Forbes, *Opt. Express* **21**, 165-171 (2013).
- [35] B. Ndagano, R. Brünig, M. McLaren, M. Duparré, and A. Forbes, *Opt. Express* **23**, 17330-17336 (2015).
- [36] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145-195 (2002).
- [37] G. Ruffato, M. Massari, and F. Romanato, *Sci. Rep.* **6**, 24760 (2016).
- [38] M. A. Cox, C. Rosales-Guzmán, M. P. J. Lavery, D. J. Versfeld, and A. Forbes, *Opt. Express* **24**, 18105-18113 (2016).

the manuscript with inputs from all the authors. A.F. supervised the project.

COMPETING FINANCIAL INTERESTS

The authors declare no financial competing interests.

MATERIALS AND CORRESPONDENCE

Correspondence and requests for materials should be addressed to A.F.

ACKNOWLEDGMENTS

We express our gratitude to Lorenzo Marrucci for providing us with q -plates and Miles Padgett and Martin Lavery for the mode sorters. B.N. acknowledges financial support from the National Research Foundation of South Africa and I. N. from the Department of Science and Technology (South Africa). B.P.G. and R.I.H. acknowledge support from CONACyT.

AUTHORS' CONTRIBUTIONS

Experiments were performed by B.N., I.N., S.S. and B.P.G. All authors contributed to the data analysis and interpretation of the results. A.F., I.N. and B.N. wrote

V. SUPPLEMENTARY INFORMATION

Sorting of scalar OAM mode. We use a compact phase element to perform a geometric transformation on OAM modes such that azimuthal phase is mapped to a transverse phase variation, i.e., a tilted wavefront. The first optical element of our OAM mode sorter performs a conformal mapping in the standard Cartesian coordinates, from a position in the input plane (x, y) to one in the output plane (u, v) , such that

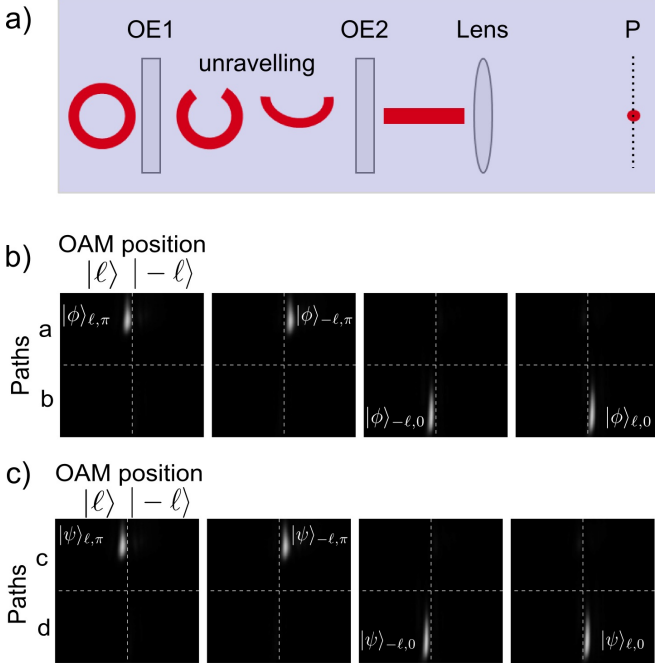


FIG. 5. **Sorting the modes.** (a) We use a mode sorter that consist of two refractive optical lenses, OE1 and OE2 which transform azimuthal phase into a linear phase and mapped onto positions. The input mode unravels after OE1 and a linear phase is retained by OE2. The phase is then mapped onto a position unique to the azimuthal charge by a Fourier lens. We use these lenses to map the modes set $(|\phi\rangle, |\psi\rangle)$ onto positions based on their orbital angular momentum system illustrated in Fig. 2 (c) and Fig. 2 (d).

$$u = \frac{d}{2\pi} \arctan\left(\frac{y}{x}\right) \quad (21)$$

$$v = -\frac{d}{2\pi} \ln\left(\frac{\sqrt{x^2 + y^2}}{b}\right) \quad (22)$$

where d is the aperture size of the free form optics and b is a scaling factor that controls the translation of the transformed beam in the u direction of the new coordinate system. The result is that after passing through a second phase-correcting optic and then a Fourier transforming lens (of focal length f), the input OAM (ℓ) is mapped to output positions (X_ℓ following

$$X_\ell = \frac{\lambda f \ell}{d}. \quad (23)$$

Crosstalk analysis. The crosstalk analysis of the vector ($|\psi\rangle$) and scalar ($|\phi\rangle$) modes is represented by a matrix of detection probabilities for each of the modes sent by Alice (rows) and measured by Bob (columns). The entries are partitioned into four quadrants: the diagonal quadrants correspond to the outcomes of measurements in matching bases while the off-diagonal show the outcomes of measurements in complementary bases.

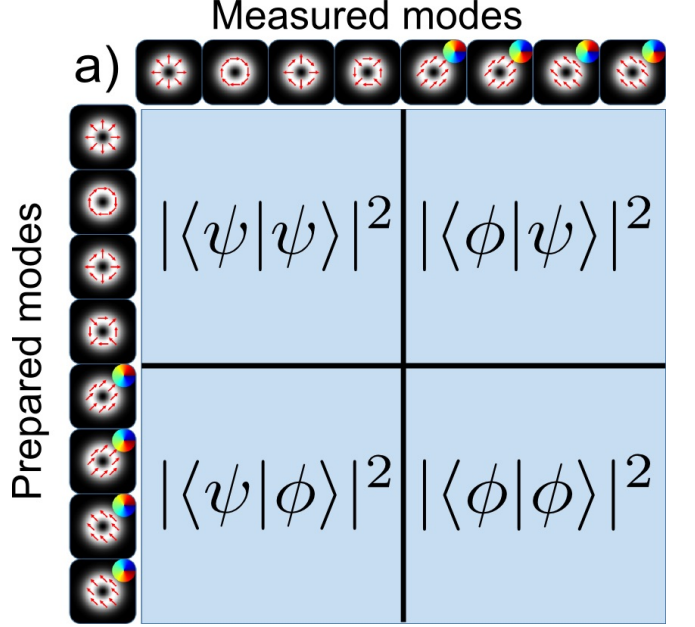


FIG. 6. **Crosstalk analysis matrix for the four dimensional sets of vector and scalar modes.** The matrix can be broken into four quadrants representing probabilities for preparation and measurements in the two basis.

Filter based detection system. The filter based detection system depends on the use of beam splitters with a combination with q -plates, wave plates and polarisers. While it is common practice for the measurement process to be identical to the generation for reversible processes – as is the case in linear optics – this approach would fail in measuring high dimensional vector mode spaces. This is because vector modes within one subset required oppositely charged q -plates. The best approach to probe the high dimensional space would require the use of beam splitters as shown in Fig. 7, however, at the cost of reducing the detection probability by a factor of $1/2$, thus halving the sift rate and secure key rate; for a key that is N -bit long, one would require sending, on average, $4N$ bits. We have tested this by building the system depicted in Fig. 7 and performing the same prepare and measure QKD protocol as detailed in the main text. For a 200 bit transmission we were only able to produce a key with 25% of the transmitted bits, as compared to 50% using the scheme described in Fig. 2 of the main text. This highlights one of the advantages of a deterministic detection system versus the probabilistic (filter-based) system.

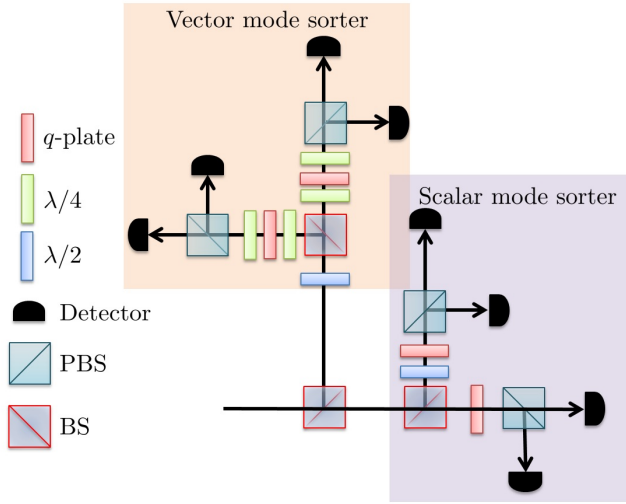


FIG. 7. **Filter based system for detecting the vector and scalar modes.** The combination of wave-plates ($\frac{\lambda}{4}$, $\frac{\lambda}{2}$), q-plates and 50/50 (BS) and polarisation (PBS) beam splitters can serve as a detection system. The wave plates can be rotated at angles shown in Table.1